CLAIMS

1. A secured and confidential method for transmitting a digital data file between a sending element and a receiving element via telecommunication or radiocommunication networks, characterized in that:
   - (steps S1, S2) the sending element (20) downloads a database (50) listing the authorized sending elements, a symmetrical fragmentation-transmission secret key (CFT);
   - (steps S3, S5) the sending element (20) transmits the fragmentation-transmission key (CFT) to the receiving element (30) via a so-called second-level relay (10);
   - (step S4) the second-level relay (10) informs the database (50) that the fragmentation-transmission key (CFT) is being used;
   - (steps S6, S7) the receiving element (20) transmits to the sending element (30) an authorization to send fragments via the second-level relay (10);
   - the sending element (20) fragments the data in the initial file, according to an incremental distribution before assignment by swapping, such that the data of each fragment is unintelligible, the level and the type of fragmentation being predefined in the fragmentation-transmission key;
   - the sending element (20) assigns each fragment an addressing path through a so-called first-level network of relays (40, 41, 42);
   - (steps S8, S9) the sending element (20) transmits each fragment to the receiving element (30) via the first-level relays (40, 41, 42);
   - the receiving element (30) reassembles the fragments received, according to the instructions in the fragmentation-transmission key (CFT), to recreate the initial data file;

- (step S10) the receiving element (30) sends an acknowledgement of receipt and of checking of the reassembly of the initial file to the database (50) via the second-level relay (10);
- (step S11) the fragmentation-transmission key (CFT) is deleted from the database (50).

2. The method as claimed in claim 1, characterized in that there are defined several different classes for defining the initial information object to be transmitted, namely:
- a class T of fragmentation types of the bit-by-bit, byte-by-byte, byte block-by-byte block, bit block-by-bit block, space-by-space type, and therefore all possible instances for each of the abovementioned types;
- a fragmentation level class F, F being a real integer at least equal to two determined when choosing the fragmentation level;
- a network size class R, R being a real integer at least equal to one, and preferably greater than or equal to two, determined when choosing the size of the network architecture;
- a class A of IP addresses of the relays of the network architecture of the types of IP addresses of the so-called first-level relays, IP addresses of the so-called second-level relays, with all possible instances.

3. The method as claimed in claim 1 or 2, characterized in that the fragmentation-transmission key (CFT) comprises two subkeys, namely:
- a fragmentation-reassembly subkey (A), unique to each initial data file to be transmitted, and for which the counting possibilities are derived from the factorial computation, comprising the instructions needed for the deletion of the

initial data file and the distribution by swapping in a set of fragments;

- a sending subkey (B), unique to each initial data file to be transmitted, and for which the counting possibilities are derived from the exponential computation, comprising the instructions needed, such as the IP addresses of the first-level relays (40, 41, 42), for routing the fragments within the network of first-level relays (40, 41, 42).

4. The method as claimed in claim 3, characterized in that the receiving element (30) addresses a request to the first-level relays (40, 41, 42), the IP address of which is contained in the sending subkey (B), to download the fragments.

5. The method as claimed in one of claims 1 to 4, characterized in that each of the first-level relays (40, 41, 42) is provided with management means for recognizing incoming fragments, intelligent sorting and forwarding the same fragments to their recipient (30).

6. The method as claimed in one of claims 1 to 5, characterized in that the second-level relay (10) is not linked to the network of first-level relays (40, 41, 42).

7. The method as claimed in one of claims 1 to 5, characterized in that the network of first-level relays (40, 41, 42) is dependent on the second-level relay (10) for the definition of readdressing tasks.

8. The method as claimed in one of claims 1 to 7, characterized in that a first-level relay (40, 41, 42) or second-level relay (10) is replaced by three in-line relays, the intermediate relay of

which is an IP address linked to the other two relays via a non-Internet connection.